BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

CLAIMS

1. A method of enabling secure transfer of a package of information in a digital communications network from a sender to a receiver, comprising the steps of:

encrypting said package of information;

providing said encrypted package of information to the receiver; and

providing to a third party an encryption key having such a format that it is unable to decrypt said package of information, said encryption key, upon positive identification of the receiver, being providable from said third party to the receiver, and enabling, with the involvement of a supplementary encryption key of the receiver, decryption of the package of information.

2. A method as claimed in claim 1, further comprising the step of providing a first encryption key, which is said supplementary encryption key, to the receiver, the encryption key provided to the third party being a second encryption key, wherein the second encryption key in combination with the first encryption key enables decryption of the package of information.

3. A method as claimed in claim 2, in which said step of encrypting said package of information further comprises the steps of:

combining said first and second encryption keys for generating a combined encryption key; and

encrypting said package of information by means of said generated combined encryption key.

4. A method as claimed in claim 2, in which said package of information is first encrypted by one of said first and second encryption keys, and then encrypted by the other one of said first and second encryption keys.

5. A method as claimed in claim 2, in which said information is encrypted by a main encryption key, said main encryption key then being divided into said first encryption key which is provided to the receiver and said second encryption key which is provided to the third party.

6. A method as claimed in claim 2, in which the step of providing a first encryption key to the receiver is preceded by the step of encrypting said first encryption key with a public key of the receiver, wherein the receiver is able to decrypt said encrypted first encryption key with a private key.

7. A method as claimed in claim 1, in which the step of providing to a third party an encryption key is preceded by the steps of:

encrypting said package of information with that encryption key; and

encrypting that encryption key, wherein said encrypted encryption key is decryptable by said supplementary encryption key of the receiver so as to enable decryption of the package of information.

8. A method as claimed in claim 7, in which said encryption key is encrypted with a public key of the receiver, and in which said supplementary encryption key is a private key of the receiver enabling decryption of said encrypted encryption key.

9. A method as claimed in claim 1, in which instructions are sent to the third party, said instructions defining under what conditions the encryption key provided to the third party may be retrieved by the receiver of the package of information.

10. A method as claimed in claim 1, in which the encryption key provided to the third party, upon instructions to the third party, is prevented from being provided to the receiver.

11. A method as claimed in claim 1, in which said receiver is identified by means of a registered certificate.

12. A method as claimed in claim 1, in which the secure transfer of said package of information is only completely performed if the sender has been identified by the third party, such as by means of a registered certificate.

13. A method as claimed in claim 1, in which a hash value derived from the contents of said package of information is stored by the third party, without storing the actual package of information, wherein the receiver will be able to detect if said package of information has been tampered with.

14. A method of enabling secure transfer of a package of information in a digital communications network from a sender to a receiver, comprising the steps of:

receiving from the sender of an encrypted package of information an encryption key which, with the involvement of a supplementary encryption key of the receiver, enables decryption of said package of information;

identifying the receiver of said package of information; and

providing said received encryption key to the receiver upon positive identification of the same.

15. A method as claimed in claim 14, in which said

supplementary encryption key is a first encryption key provided to the receiver, and in which the encryption key received in the step of receiving an encryption key is a second encryption key, the combination of said first and second encryption keys enabling decryption of said package of information.

16. A method as claimed in claim 14, in which the encryption key received in the step of receiving an encryption key is an encrypted encryption key.

17. A method as claimed in claim 16, in which said encryption key is encrypted with a public key of the receiver, and in which said supplementary encryption key is a private key of the receiver enabling decryption of said encrypted encryption key.

18. A method as claimed in claim 14, in which instructions are received from the sender, said instructions defining under what conditions the encryption key received from the sender may be retrieved by the receiver of the package of information.

19. A method as claimed in claim 14, in which the receiver is identified by means of a registered certificate.

20. A method as claimed in claims 14, further comprising the step of identifying the sender, wherein the secure transfer of said package of information is only completely performed if the sender has been identified, such as by means of a registered certificate.

21. A method as claimed in any one of claims 14, further comprising the step of storing a hash value derived from the contents of said package of information, without storing the actual package of information,

wherein the receiver will be able to detect if said package of information has been tampered with.

22. A method of enabling secure transfer of a package of information in a digital communications network from a sender to a receiver, comprising the steps of:

obtaining said package of information, which is encrypted, from the sender;

being positively identified by a third party;

obtaining from said third party an encryption key having such a format that it is unable to decrypt said package of information, said third party having obtained the encryption key from the sender; and

decrypting said package of information by means of said obtained encryption key with the involvement of a supplementary encryption key.

23. A method as claimed in claim 22, further comprising the step of obtaining a first encryption key, which is said supplementary encryption key, from the sender, the encryption key obtained from the third party being a second encryption key, wherein the step of decrypting said package of information comprises the step of combining the first encryption key and the second encryption key.

24. A method as claimed in claim 23, in which said step of decrypting said package of information further comprises the steps of:

combining said first and second encryption keys for generating a combined encryption key; and

decrypting said package of information by means of said generated combined encryption key.

25. A method as claimed in claim 23, in which said package of information is first decrypted by one of said

first and second encryption keys, and then decrypted by the other one of said first and second encryption keys.

26. A method as claimed in claim 23, in which said first encryption key is encrypted with a public key of the receiver, wherein said step of decrypting said package of information is preceded by the step of decrypting said encrypted first encryption key with a private key.

27. A method as claimed in claim 22, in which the encryption key obtained from the third party is encrypted, wherein the step of decrypting said package of information comprises the steps of:

decrypting the encrypted encryption key obtained from the third party by means of said supplementary encryption key; and

decrypting said package of information with the decrypted encryption key.

28. A method as claimed in claim 27, in which the encryption key obtained from the third party is encrypted with a public key of the receiver, wherein said supplementary encryption key is a private key of the receiver enabling decryption of the encrypted encryption key.

29. A method as claimed in claim 22, in which the step of being positively identified by a third party comprises identification by means of a registered certificate.

30. A method as claimed in claim 22, further comprising the steps of:

obtaining from the third party a first hash value which has been derived from the contents of said package of information by means of a hash function;

calculating by means of said hash function a second hash value of the obtained package of information; and

comparing said first hash value with said second hash value, in order to detect if said package of information has been tampered with.

31. A system for enabling secure transfer of a package of information in a digital communications network from a sender to a receiver, comprising means for performing the steps in the methods as claimed in claim 1.

32. A computer readable medium for enabling secure transfer of a package of information in a digital communications network from a sender to a receiver, comprising means for performing the steps in the method as claimed in claim 1.